大同大學叢書

數論初步

吳在

數論初步

大同大學叢書

民國二十一年一月二十九日敝公司突遭國難總務處印刷所編譯所書棧房均被炸燬附設之涵芬樓東方圖書館尚公小學亦遭殃及盡付焚如三十五載之經營隳於一旦迭蒙各界慰問督望速圖恢復詞意懇摯銜感何窮敝館雖處境艱困不敢不勉爲其難因將需用較切各書先行覆印其他各書亦將次第出版惟是圖版裝製不能盡如原式事勢所限想荷鑒原謹布下忱統祈垂督

上海商務印書館謹啓

中華民國二十年二月初版
民國廿一年九月印行國難後第一版

(一〇二六)

大同大學叢書 數論初步一冊

每冊定價大洋壹元陸角
外埠酌加運費匯費

編輯者 吳在淵
校訂者 吳敦復 華綰言
發行人 王雲五 上海河南路
印刷者 商務印書館 上海河南路
發行所 商務印書館 上海及各埠

數論初步

序

間嘗聞言:方今我國青年求知之慾甚於飢渴;私心竊喜,以爲學殖進步之速當可操券待矣.起視出版界,乃不禁爽然,小說出品,斗量車載;科學書籍,寥若晨星,其高深者尤難一二覯,是何也?商家本爲貨殖,供自應乎所求,陽春之和難求,資本時虞虛擲,卽有名作,未敢發行,而能載筆著述者又多寒士,腹笥雖富,僅足資生,知音之難,千古同慨,抱璞途泣,是其恆情,斯所以科學高深之作,絕跡於市也;然則柰何?曰:欲人多能知樂,必先使能操絃;欲人多能調羹,必先使能識味,青年求知之慾固在,必有以善導而養之,庶能充其量於正軌乎.

本書編輯之目的,卽在以整數論初步介紹於青年,力以平易爲主,凡理論之接近於高中數學程度者,儘量採用之.其較高部分,如代數,數等分圓周問題,Galois 氏虛數,級數形式,等,凡適當發展之各需有可觀之卷帙者概從割愛.每卷更附若干問題,以便初學之練習,學者倘能由此引起興趣而進求專書,則本書已不爲無補矣.

整數論一科,在實用方面尚無甚應用.此或與我國學界崇實主義之潮流不合.然數學之正軌,實在理論精嚴及運思深入,應用為後起之事,今日無者他日或有,如昔之非歐幾里得幾何然,不足為此科病也.

抑 Gauss 氏有言曰:「數學乃科學中之女王,而整數論又為數學中之女王」,整數論之莊嚴昳麗,儀態萬方,可於此語中得之.古來諸數學大家必有一時沉醉此中,則此科之價值從可知矣.

不佞粗疏譾陋,罣一漏萬,在所不免,甚望藉此拋磚引玉,得邦之彥碩有博大宏深之著作繼出為幸.

中華民國十九年七月吳在淵識.

數論初步

目錄

第一章 整數之初等性質

第二章 等餘之理論

第三章 等餘式解法

第四章　平方賸餘

第五章 不定方程式

附 錄

數論初步

第一章　整數之初等性質

1. 基本概念及規律. 正整數,即

$$1,\ 2,\ 3,\ 4,\ 5,\ \cdots\cdots\cdots\cdots\cdots$$

名之曰自然數. 本章所論爲自然數之某種初等性質.爲便利起見,當無混淆之慮時,恆用整數或數等語以表自然數.

吾人於此假定整數之意義,以及大於,小於,等於,和,差,積,等之意義,皆爲學者所已知.

從如此所假定爲已知之概念及定義可徑得下之諸定理:

定理一. 任意二整數之和爲一整數.

定理二. 任意二整數之差爲一整數.

定理三. 任意二整數之積爲一整數.

其餘基本定理吾人所不必證者,包括之於下諸公式中:

定理四. $a+b=b+a.$

定理五. $a\times b=b\times a.$

定理六. $(a+b)+c=a+(b+c)$.

定理七. $(a\times b)\times c=a\times(b\times c)$.

定理八. $a\times(b+c)=a\times b+a\times c$.

此中 a, b, c 表任意自然數.

例題一

(1) 證下諸關係式:

$$1+2+3+\cdots\cdots\cdots\cdots+n=\frac{1}{2}n(n+1),$$

$$1+3+5+\cdots\cdots\cdots\cdots+(2n-1)=n^2,$$

$$1^3+2^3+3^3+\cdots\cdots\cdots\cdots+n^3=\left(\frac{1}{2}n(n+1)\right)^2$$
$$=(1+2+3+\cdots+n)^2.$$

(2) 求下各級數之和:

$$1^2+2^2+3^2+\cdots\cdots\cdots\cdots+n^2$$

$$1^2+3^2+5^2+\cdots\cdots\cdots\cdots+(2n-1)^2,$$

$$1^3+3^3+5^3+\cdots\cdots\cdots\cdots+(2n-1)^3,$$

(3) 從諸方程式:

$1^2=0+1,\quad 2^2=1+3,\quad 3^2=3+6,\quad 4^2=6+10,\cdots\cdots;$

及諸方程式:

$1=1^3,\quad 3+5=2^3,\quad 7+9+11=3^3,\quad 13+15+17+19=4^3,$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots;$

發見及建設其規律.

2. 約數及倍數. 單位.

定義. 一整數 a 能以一整數 b 除盡之者,謂有一整數 c, 能使 $a=bc$ 也.

從此定義,顯然可知 a 亦能以 c 除盡.

二整數 b 及 c 謂爲 a 之約數,或曰因數,而謂 a 爲 b 或 c 之倍數.

求二整數 b 及 c 使 bc 等於一所設整數 a 之方法,曰析因數法,亦曰以 a 析成因數.

定理一. 若 b 爲 a 之一約數,及 c 爲 b 之一約數,則 c 爲 a 之一約數.

因 b 爲 a 之一約數,則有一整數 β 使 $a=b\beta$. 因 c 爲 b 之一約數,則有一整數 γ 使 $b=c\gamma$. 以此 b 之值代入上一式中,得 $a=c\gamma\beta$. 但從前款定理三,知 $\gamma\beta$ 爲一整數;由是 c 爲 a 之一約數,而本定理已證明矣.

此定理亦可如下述之:

一數之約數亦爲其倍數之約數,或一數之倍數亦爲其約數之倍數.

定理二. 若 c 爲 a 及 b 二者之約數,則 c 爲 a 及 b 和或差,即 $a\pm b$, 之約數.

從定理之假設,知有二整數 α 及 β, 使

$$a=c\alpha, \qquad b=c\beta.$$

加或減之,得

$$a\pm b=c\alpha\pm c\beta=c(\alpha\pm\beta)=c\delta.$$

此中 δ 為一整數.由是 c 為 $a\pm b$ 之約數.

定理三. 若 c 為 a 及 b 之約數,又 p 及 q 為任意整數,則 c 為 $pa+qb$ 之約數.

證法與前定理之證相類,茲從略.

定理四. a 為一整數,則一切整數恆可以如下諸式之一表之:

$$am,\quad am+1,\quad am+2,\quad \cdots\cdots,\quad am+a-1.$$

但此中 m 之值為一整數.

設任取一整數為 N,則此 N 或為 a 之倍數或非 a 之倍數,二者必居其一. 若 N 為 a 之倍數,則 N 可以 am 表之;若 N 非 a 之倍數,則在 N 中減去 a 之整倍數 am 以後必有小於 a 之賸餘,此賸餘必為 $1, 2, 3, \cdots\cdots, a-1$ 中之一,故 N 恆可以

$$am+1,\quad am+2,\quad \cdots\cdots,\quad am+a-1$$

之一表之.

觀察約數之方法. 在普通算術中有觀察約數之方法數事,今舉之於下,其證學者可自為之:

(I) 凡數之一位數字為 2 之倍數者,此數必有 2 之

約數.

(II) 凡數之一位數字爲 5 之倍數者,此數必有 5 之約數.

(III) 凡數之十位及一位共二位數爲 4 之倍數者,此數必有 4 之約數.

(IV) 凡數之十位及一位共二位數爲 25 之倍數者,此數必有 25 之約數.

(V) 凡數之各位數字和爲 9 之倍數者,此數必有 9 之約數.

(VI) 凡數之各位數字和爲 3 之倍數者,此數必有 3 之約數.

(VII) 凡數中奇位數字和與偶位數字和之差爲 11 之倍數者,此數必有 11 之約數.

定義. 若 a 及 b 皆能以 c 除盡,則謂 c 爲 a 及 b 之公約數,或公因數

凡二個整數恆有一公約數 1.

能除盡 a 及 b 之最大整數名之曰 a 及 b 之最大公約數.擴而充之,吾人可照此法定 n 個整數 $a_1, a_2, a_3, \cdots\cdots\cdots, a_n$ 之公約數及最大公約數.

定義. 若一整數 a 爲二個或多個整數之倍數,則名 a 爲諸整數之公倍數.

一整數爲二個或多個整數之倍數而最小者爲其最小公倍數.

整數 1 爲一切整數之約數,爲一切整數約數之整數僅有此 1,此皆顯然可知者.名此 1 曰單位 (Unit).

定義. 二個或多個整數除 1 外無公約數者名之曰互素 (to be prime to each other).

定義. 若一組整數其中任意二數無 1 以外之公約數者,謂此一組整數互素.

例 題 二

(1) 若 n 爲正整數,證 n^3-n 可以 6 除盡之.

(2) 四個連續整數之積加 1,則其和爲一完全平方數.證之.

(3) n 爲正整數時,示 $2^{4n+2}+1$ 有一異於本身及 1 之因數.

(4) 一整數之平方必爲以下各形式之一:

(a) $3m$, $3m+1$;

(b) $4m$, $4m+1$;

(c) $5m$, $5m\pm1$.

證之.

(5) 已知 62※※427 爲 99 之倍數,求在※※二位置

之數字.

3. 素數. **定義.** 若一整數 p 與 1 異而除本身及 1 以外無他約數,則謂此數爲素數 (Prime number or Prime).

定義. 一整數至少有一個約數異於本身及 1 者謂之曰合成數(Composite number or Composite).

於是一切整數分成三類:

(a)　單位;

(b)　素數;

(c)　合成數.

吾人已見第一類僅含一個數.第三類顯然含有無窮個數;由其含有 $2^2, 2^3, 2^4, \cdots\cdots$ 卽可見之.至次款中,吾人當見第二類亦含有無窮個數.

定義. 一合成數 N 可分成一雙因數 m, n, 卽 $N=mn$, 則謂此 m 及 n 爲 N 之互補約數,或曰互補因數.

於是,素數僅有一雙互補約數爲其本身及 1, 卽

$$N = 1. N.$$

合成數至少有二雙互補約數,如

$$N=1. N=m_1. n_1=m_2. n_2=\cdots\cdots.$$

若　$1<m_1<m_2<\cdots\cdots,$

則　$N>n_1>n_2>\cdots\cdots.$

故以 N 之約數依從小至大之次序列之.則可得

$$1<m_1<m_2<\cdots\cdots<n_2<n_1<N.$$

定義. 凡約數之爲素數者名之曰素約數,或曰素因數.

定理一. 凡大於1之自然數至少有一個素約數.

令N爲大於1之任意整數.

若N爲一素數,則N本身卽爲其素約數.

若N爲一合成數,則必至少有二雙互補約數,如

$$N=1.N=m_1.n_1=\cdots\cdots,$$

假定此中 $1<m_1<\cdots\cdots<n_1<N$,

卽m_1爲1以外N之最小約數.然則m_1必爲N之素約數.何則,如云m_1爲合成數,則m_1必有比其本身小而非1之約數,而此約數亦必爲N之約數,則是m_1非1以外N之最小約數矣;與假定矛盾,不可也.

定理至此已證明矣.

定理二. N爲任意整數,I爲平方等於N之數(不必爲整數),若N無一小於或等於I之素因數,則N爲一素數.

假定N爲合成數,m, n爲其任意一雙互補約數,而$m<n$.

從定理之假設, $m>I$,

故必 $n>I$, 而 $m.n>I^2$.

然 $I^2=N$,

故 $m.n>N$,

由是假定之 $N=m.n$ 不合理.